Discrete Mathematics 123 (1993) 151–177
North-Holland

Cyclic near difference sets of type 1

Wan-Di Wei and Shuhong Gao
Department of Mathematics, Sichuan University, Chengdu 610064, China

Benfu Yang
Department of Mathematics, Teacher-Training College of Chengdu, Chengdu, China

Received 3 August 1990

Abstract

Some nonexistence theorems for cyclic near difference sets of type 1 are established, some cyclic near difference sets of type 1 are constructed, and the uniqueness of (v, k, λ) cyclic near difference sets is proved for some triples (v, k, λ).

1. Introduction

In 1973, Ryser [10] proposed and studied two types of 'almost' cyclic difference sets, which were called the cyclic near difference sets of type 1 and the cyclic near difference sets of type 2, respectively. He obtained some nonexistence theorems and examples for near difference sets. In [11], we have obtained some results for the cyclic near difference sets of type 2. In the present paper, we will study the cyclic near difference sets of type 1.

Let $v \geqslant 4$ be an even integer, and k, λ positive integers. Suppose that $D = \{a_1, a_2, \ldots, a_k\}$ is a set of k residues modulo v with the property that for any residue $a \not\equiv 0, v/2 \pmod v$, the congruence equation

$$a_i - a_j \equiv a \pmod v, \quad a_i, a_j \in D$$

has exactly λ solution pairs (a_i, a_j) and no solution pair for the residue $a \equiv v/2 \pmod v$. Then D is called a (v, k, λ) cyclic near difference set of type 1, and $n := k - \lambda$ is called the order of D. Hereafter we exclusively deal with the cyclic near difference sets of type 1, so they are simply called near difference sets. A $(v, k, 1)$ cyclic near difference set is called a planar near difference set. Two (v, k, λ) near difference sets D_1 and D_2 are said to be equivalent if there are integers s and t $(\gcd(t, v) = 1)$ such that $D_1 = tD_2 + s$. It is clear that if there exists a (v, k, λ) cyclic near difference set, then

$$\lambda(v-2) = k(k-1).$$

It is also clear that a (v, k, λ) near difference set is in fact a special relative difference set, i.e. an $(m, n; k; \lambda_1, \lambda_2)$ cyclic relative difference set with $m = v/2$, $n = 2$, $\lambda_1 = 0$, and $\lambda_2 = \lambda$. Cyclic relative difference sets have been extensively studied (see, for example, [3, 6]). Although the study of relative difference sets appeared much earlier than that of near difference sets, Ryser did not point out the relationship between relative difference sets and near difference sets.

The nonexistence theorem established by Ryser reads as follows.

Theorem 1.1 (Ryser [10]). *Let D be a (v, k, λ) near difference set. Then* (i) $v \equiv 0 \pmod 4$ *implies that $K - 2\lambda$ is a square,* (ii) $v \equiv 2 \pmod 4$ *implies that k is a square,* (iii) *there exists a $(v/2, k, 2\lambda)$ cyclic difference set (possibly degenerate).*

The purpose of this paper is: (1) providing a simpler proof and a finer statement of Theorem 1.1, (2) establishing some new non-existence theorems for near difference sets, (3) studying the existence problem for some type of near difference sets. In order to do so, we first present some known results, some of these come from the theory of relative difference sets, and the others from the theory of Diophantine equations.

2. Some known results

We need the following (known) results on abelian relative difference sets.

Theorem 2.1 (Ko and Ray-Chaudhuri [6]). *For an $(m, n; k; 0, \lambda)$ relative difference set in an abelian group G with exponent v^*, an integer t is a multiplier if* (i) $k = k_1 k_2$, $\gcd(k_1, v^*) = 1$, $k_1 > \lambda$, (ii) *for each prime p dividing k_1, $t \equiv p^{f_p} \pmod{v^*}$ for some nonnegative integer f_p.*

Theorem 2.2 (McFarland and Rice [7]). *Let D be an $(m, n; k; \lambda_1, \lambda_2)$ abelian difference set, t a multiplier of D. Then there exists a translate of D which is fixed by t.*

Noting that $k > 1$, by Theorem 5.2 in [5] we have the following theorem.

Theorem 2.3. *For any near difference sets, -1 is not a multiplier.*

We also need the following results from Diophantine equations. Catlan proposed in 1842 the following conjecture (see, for example, Mordell [8]).

Catlan's Conjecture: The only solution in integers of the equation

$$x^e - y^f = 1, \quad x, y, e, f > 1$$

is

$$f = x = 3, \quad e = y = 2.$$

An alternative form of the conjecture is the following.
If p and q are primes, then a similar result holds for

$$x^p - y^q = 1, \quad x, y > 1.$$

This conjecture still remains open. But some results known about it serve our purpose.

Theorem 2.4 (Cassels [2]). *The Diophantine equation*

$$y^2 + 1 = x^e, \quad x, y, e > 1$$

has no solutions in integers.

Theorem 2.5 (Ko [5]). *The only solution of the Diophantine equation*

$$x^2 - 1 = y^f, \quad x, y, f > 1$$

is

$$x = f = 3, \qquad y = 2.$$

3. Nonexistence theorems

We first give a simpler proof of Theorem 1.1. Let $D = \{a_1, a_2, \ldots, a_k\}$ be a (v, k, λ) near difference set, and

$$\theta(x) := \theta_D(x) \equiv x^{a_1} + x^{a_2} + \cdots + x^{a_k} \pmod{x^v - 1}$$

the Hall polynormal of D. Then

$$\begin{aligned} \theta(x)\theta(x^{-1}) &\equiv k + \lambda(x + x^2 + \cdots + x^{(v/2)-1} + x^{(v/2)+1} + \cdots x^{v-1}) \\ &\equiv k + \lambda(1 + x^{(v/2)})(x + x^2 + \cdots + x^{(v/2)-1}) \pmod{x^v - 1}. \end{aligned} \tag{3.1}$$

Setting $x = -1$ in (3.1), we have

$$\begin{aligned} (\theta(-1))^2 &= k + (1 + (-1)^{(v/2)})(-1 + 1 - 1 + \cdots + (-1)^{(v/2)-1})\lambda \\ &= \begin{cases} k, & \text{if } v \equiv 2 \pmod 4, \\ k - 2\lambda, & \text{if } v \equiv 0 \pmod 4. \end{cases} \end{aligned} \tag{3.2}$$

Let m_0 be the number of even elements in D, and m_1 the number of odd elements in D. Then

$$(\theta(-1))^2 = (m_0 - m_1)^2.$$

By (3.1), we have

$$\theta(x)\theta(x^{-1}) \equiv k + 2\lambda(x + x^2 + \cdots + x^{(v/2)-1}) \equiv k - 2\lambda + 2\lambda T_1(x) \pmod{x^{v/2} - 1}, \tag{3.3}$$

where

$$T_1(x) \equiv 1 + x + \cdots + x^{(v/2)-1} \pmod{x^{v/2} - 1}.$$

On the other hand, since $v/2 \not\equiv a_i - a_j \pmod{v}$, it follows that

$$a_i \not\equiv a_j \pmod{v/2} \quad (1 \leqslant i < j < k).$$

Hence D is a $(v/2, k, 2\lambda)$ cyclic difference set (possibly degenerate). Summing up, Theorem 1.1 has been proved in a different and simpler way, and can be stated more specifically.

Theorem 3.1. *If there exists a (v, k, λ) near difference set, then* (i) *k is the square of the difference of the number of even elements and the number of odd elements when $v \equiv 2 \pmod 4$,* (ii) *$k - 2\lambda$ is the square of the difference of the number of even elements and the number of odd elements when $v \equiv 0 \pmod 4$, and* (iii) *there exists a $(v/2, k, 2\lambda)$ cyclic difference set (possibly degenerate).*

Denote by $n_i\ (0 \leqslant i \leqslant 3)$ the number of elements in D such that $a_j \equiv i \pmod 4$. Then we can prove the following theorem.

Theorem 3.2. *Suppose D is a (v, k, λ) near difference set. Then when $v \equiv 4 \pmod 8$, the parameter k is a sum of two squares:*

$$k = (n_0 - n_2)^2 + (n_1 - n_3)^2. \tag{3.4}$$

Proof. Clearly,

$$\theta(i)\theta(i^{-1}) = ((n_0 - n_2) + (n_1 - n_3)i)((n_0 - n_2) - (n_1 - n_3)i) = (n_0 - n_2)^2 + (n_1 - n_3)^2. \tag{3.5}$$

On the other hand,

$$[k + \lambda(1 + x^{(v/2)})(x + x^2 + \cdots + x^{(v/2)-1})]_{x=i} = k, \quad \text{if } v \equiv 4 \pmod 8. \tag{3.6}$$

Combining (3.1), (3.5) and (3.6), we complete the proof. □

As a consequence of Theorem 3.2, we have the following corollary.

Corollary 3.3. *Let v, k and λ be positive integers. If $v \equiv 4 \pmod 8$ and if there exists a prime $p \equiv 3 \pmod 4$ such that $p^{2c-1} \| k$ for some positive integer c, then (v, k, λ) near difference set does not exist.*

According to this corollary, we assert, for example, that there do not exist planar near difference sets of order 65. The reason is as follows. When $n=65$, $n\equiv 1 \pmod 8$ and $v\equiv 4 \pmod 8$. On the other hand, $k=n+1=66$, and $3 \parallel 66$.

Theorem 3.4. *If D is a (v,k,λ) near difference set, then $k\leqslant v/2$.*

Proof. We pair the elements of Z_v as follows:

$$\begin{Bmatrix}0\\v/2,\end{Bmatrix}\ \begin{Bmatrix}1\\v/2+1,\end{Bmatrix}\ \ldots,\ \begin{Bmatrix}i\\v/2+i,\end{Bmatrix}\ \ldots,\ \begin{Bmatrix}v/2-1\\v-1\end{Bmatrix}$$

Since $v/2\equiv a_i-a_j \pmod v$ has no solutions (a_i,a_j) with $a_i,a_j\in D$, D contains at most one element of each pair. Hence the theorem. □

4. Planar near difference sets

In this section we concentrate our discussion on the planar difference sets. From Theorem 3.2 we easily obtain the following theorem.

Theorem 4.1. *If there exists a planar near difference set of order n, then n is not of the form*

$$n=m^g, \quad m,g>1. \tag{4.1}$$

Proof. By (1) we have, $v=n^2+n+2$. Then

$$v\equiv\begin{cases}0 \pmod 4, & \text{if } n\equiv 1 \text{ or } 2 \pmod 4,\\ 2 \pmod 4, & \text{if } n\equiv 0 \text{ or } 3 \pmod 4.\end{cases}$$

By Theorem 1.1 we know that when $n\equiv 1$ or $2 \pmod 4$

$$n-1=k-2=z^2 \qquad \text{for some integer } z, \tag{4.2}$$

and that when $n\equiv 0$ or $3 \pmod 4$,

$$n+1=k=w^2 \quad \text{for some integer } w. \tag{4.3}$$

If n is of the form (4.1), then (4.2) is impossible and (4.3) holds if

$$m=2, \qquad g=3, \qquad w=3$$

i.e.

$$n=8, \qquad k=9, \qquad v=74.$$

We now assert that there are no planar near difference sets of order 8. Suppose that the contrary is true and D is such a difference set. Then Theorem 2.1 implies that 3 is a multiplier of D. Since $3^9\equiv -1 \pmod{74}$, -1 is also a multiplier of D. This is impossible by Theorem 2.3. This completes the proof. □

For $m=1$, i.e. $n=1$, there certainly exists a planar near difference set of order 1, which was given by Ryser in [10]:

$$D=\{0,1\}\ (\mathrm{mod}\ 4).$$

Let p be a prime. It is well known that for any prime power p^α there exists a cyclic planar difference set of order p^α. But the following Theorem shows that for planar near difference sets, the conclusion is quite different.

Theorem 4.2. *Let p^α be a prime power, and let there be a near planar difference set of order p^α. Then*

$$\alpha=1 \quad \textit{and} \quad p=2,\ 3 \text{ or } 4x^2+1 \tag{4.4}$$

for some integer x.

Proof. Since $n=p^\alpha$, Theorem 4.1 implies that $\alpha=1$. When $p\equiv 1\ (\mathrm{mod}\ 4)$, $p-1$ must be a square by Theorem 1.1, so p is of the form $4x^2+1$. When $p\equiv 2\ (\mathrm{mod}\ 4)$, p must be 2. When $p\equiv 3\ (\mathrm{mod}\ 4)$, (4.3) gives

$$p=(w+1)(w-1).$$

but

$$(w-1)(w+1)\begin{cases}\text{is not a prime,} & \text{if } w>2,\\ =3, & \text{if } w=2.\end{cases}$$

Thus p must be 3. This completes the proof. □

For the cases $p=2$ and 3, there certainly exist planar near difference sets of these orders, which were given by Ryser in [10]:

$$D_2=\{0,1,3\}\ (\mathrm{mod}\ 8),$$

$$D_3=\{0,1,4,6\}\ (\mathrm{mod}\ 14).$$

According to Theorem 1.1, if there exists a planar near difference set of order n, then

$$n=\begin{cases}w^2-1, & \text{when } v\equiv 2\ (\mathrm{mod}\ 4),\\ z^2+1, & \text{when } v\equiv 0\ (\mathrm{mod}\ 4)\end{cases}$$

for some integer w and z. We can now prove the following theorem.

Theorem 4.3. *If* (1) $z\equiv 4\ (\mathrm{mod}\ 8)$, (2) $p\equiv 3\ (\mathrm{mod}\ 4)$ *is a prime, and* (3) $p^{2c-1}\,\|\,(z^2+2)$ *for some positive integer c, then there is no planar near difference set of order z^2+1.*

Proof. Let $n=z^2+1$. Then $k=z^2+2$. When $z\equiv 4\ (\mathrm{mod}\ 8)$,

$$v\equiv n(n+1)+2\equiv(z^2+1)(z^2+2)+2\equiv 4\ (\mathrm{mod}\ 8).$$

According to Corollary 3.3 there is no planar near difference set of order z^2+1. □

Theorem 4.4. *Let* $1 \leqslant n < 5002$. *There exist planar near difference sets of order n if and only if* $1 \leqslant n \leqslant 3$.

Proof. Suppose that there exist planar near difference sets of order n. By Theorem 1.1(iii) there exist $((1/2)n(n+1)+1, n+1, 2)$ cyclic difference sets. Such difference sets are divided into three categories:

(1) Nontrivial cyclic difference sets with $n+1 \leqslant ((n(n+1)/2)+1)$: Theorem 3.4 of Hughes [4] and Table 1 of Baumert [1], the parameters (v, k, λ) of these cyclic difference sets are given only by

$$(v, k, \lambda) = (11, 5, 2), (37, 9, 2). \tag{4.5}$$

(2) The complements of nontrivial (v', k', λ') cyclic difference sets with $k \leqslant v/2$: In this case, $v' + \lambda' - 2k' = 2$. Then $v' - 2k' = 1$ and $\lambda' = 1$. Therefore

$$(v, k, \lambda) = (7, 4, 2) \tag{4.6}$$

which implies that $(v', k', \lambda') = (7, 3, 1)$.

(3) Trivial cyclic difference sets with parameters $(v, v-1, 2)$ or $(v, v, 2)$. Then

$$(v, k, \lambda) = (4, 3, 2), (2, 2, 2). \tag{4.7}$$

The parameters (v^*, k^*, λ^*) of near difference sets corresponding to the cyclic difference sets with the parameters in (4.5)–(4.7) are given by

$$(v^*, k^*, \lambda^*) = (22, 5, 1), (74, 9, 1), (14, 4, 1), (8, 3, 1), (4, 2, 1).$$

The planar near difference sets with parameters $(14, 4, 1)$, $(8, 3, 1)$ and $(4, 2, 1)$ were constructed by Ryser [10], and these were provided above. The nonexistence of planar $(74, 9, 1)$ near difference sets has been given in the proof of Theorem 4.1. Since $22 \equiv 2 \pmod 4$ and 5 is not a square, it follows from Theorem 1.1 that there are no planar $(22, 5, 1)$ near difference sets. This completes the proof. □

5. $(4\lambda, 2\lambda, \lambda)$ near difference sets

Let D be a (v, k, λ) near difference set. By Theorem 3.4 we have $k \leqslant v/2$. In this section we will deal with the critical case $k = v/2$. In this case we have $\lambda = v/4$ by the basic relation $\lambda(v-2) = k(k-1)$, so

$$(v, k, \lambda) = (4\lambda, 2\lambda, \lambda).$$

Theorem 5.1. *There exist* $(4\lambda, 2\lambda, \lambda)$ *near difference sets if and only if* $\lambda = 1$.

Proof. When $\lambda = 1$, we know that $\{0, 1\}$ is a $(4, 2, 1)$ near difference set. From now on we suppose that $\lambda \geqslant 2$ and D is a $(4\lambda, 2\lambda, \lambda)$ near difference set in $Z_{4\lambda}$. Then D contains

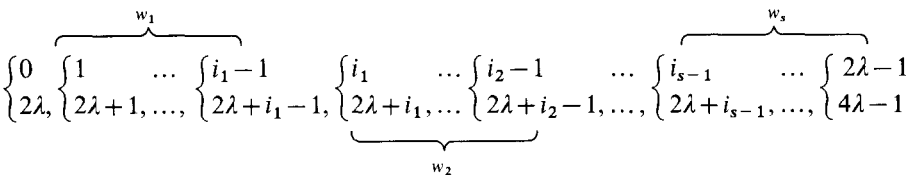


Fig. 1.

exactly one element of each of the following pairs:

$$\begin{Bmatrix}0\\2\lambda,\end{Bmatrix}\ \begin{Bmatrix}1\\2\lambda+1,\end{Bmatrix}\ \begin{Bmatrix}2\\2\lambda+2,\end{Bmatrix}\ \ldots\ \begin{Bmatrix}2\lambda-1\\4\lambda-1.\end{Bmatrix}$$

Without loss of generality, we may assume 'that $0\in D$ and $4\lambda-1\notin D$. Considering the maximal segments of consecutive integers in D, we display D in Fig. 1 which indicates that $D=\{0,1,\ldots,i_1-1\}\cup\{2\lambda+i_1,\ldots,2\lambda+i_2-1\}\cup\cdots\cup\{i_{s-1},\ i_{s-1}+1,\ldots,\ 2\lambda-1\}$, where $0=i_0<i_1<i_2<\cdots<i_{s-1}\leqslant i_s=2\lambda$ and $w_j=i_j-i_{j-1}$, $1\leqslant j\leqslant s$. It is easily seen from Fig. 1 that s must be odd. Noting that $\sum_{i=1}^{s}(W_i-1)$ is just the number λ of occurrences of 1 in the difference list of D and $\sum w_i=|D|=2\lambda$, we have $\lambda=\sum_{i=1}^{s}(W_i-1)=2\lambda-s$. So $\lambda=s$ is odd.

Let D_1 (D_2) be the set of even numbers (odd numbers) in D, and λ_1 (λ_2) the number of occurrences of 2 in the difference list of D, (D_2). Then $\lambda=\lambda_1+\lambda_2$. Fig. 2 displays D if $2\lambda-2$ belongs to D_1. Fig. 3 displays D of $2\lambda-2$ does not belong to D_1.

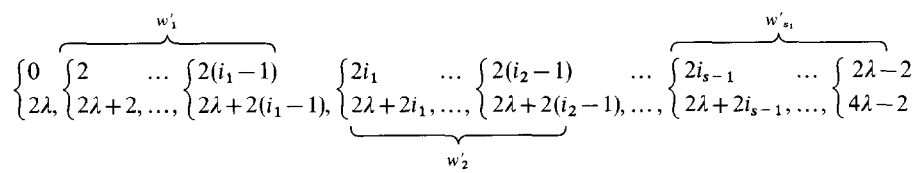


Fig. 2.

or

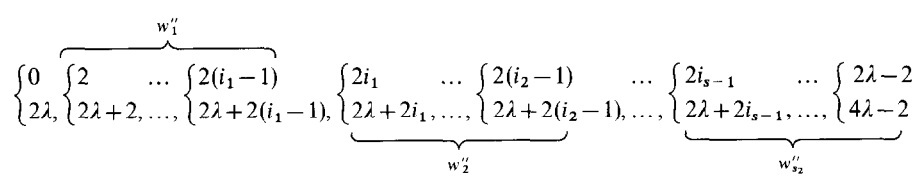


Fig. 3.

where $\sum w_i'=\lambda=\sum w_i''$. Then s_1 is odd and s_2 is even. If the former is true, we have

$$\lambda_1=\sum_{i=1}^{s_1}(w_i'-1)=\lambda-s_1,$$

if the latter is true, we have

$$\lambda_1 = \sum_{i=1}^{s_2} (w_i'' - 1) + 1 = \lambda - s_2 + 1.$$

Therefore, λ_1 is even in both cases. By a similar argument we can show that λ_2 is also even. Hence, $\lambda = \lambda_1 + \lambda_2$ is even, a contradiction.

6. $(4(\lambda+1), 2\lambda+1, \lambda)$ near difference sets

In this section we study the case $k = v/2 - 1$. Then the parameters are

$$(v, k, \lambda) = (4(\lambda+1), 2\lambda+1, \lambda). \tag{6.1}$$

For this family of near difference sets, Ko and Ray-Chandhuri [6] have given two examples:

$(12, 5, 2)$: $\{1, 3, 4, 5, 8\}$

$(16, 7, 3)$: $\{0, 1, 2, 7, 11, 13, 14\}$

They asserted in Table 1 of [4] that there are neither $(8, 3, 1)$ near difference sets nor $(20, 9, 4)$ near difference sets. However, Ryser [10], as we have mentioned above, has given a $(8, 3, 1)$ near difference set, and in the following we will give a $(20, 9, 4)$ near difference set. Furthermore, we will investigate the number, $N(v, k, \lambda)$, of different (v, k, λ) near difference sets, and prove the results given in Table 1.

We first give some general observations. Suppose that there exists a $(4(\lambda+1), 2\lambda+1, \lambda)$ near difference set, say D, and let t be a multiplier of D. By Theorem 2.2, we may assume that D is fixed by t in constructing D. Then D must be a union of some of the orbits of Z_v under the permutation: $x \to tx$.

Assume that $k = 2\lambda+1$ is a prime. By Theorem 2.1, $t = k$ is a multiplier of D. Since $t^2 \equiv 4\lambda^2 + 4\lambda + 1 \equiv 1 \pmod{v}$ the length of each orbit of Z_v under the permutation $x \to tx$ is less than or equal to 2. The orbits are of the form $a\{1, 2\lambda+1\} = \{a, (2\lambda+1)a\}$, $a \in Z_v$. Clearly, $a\{1, 2\lambda+1\} + 2\lambda + 2 \equiv (a + 2\lambda + 2)\{1, 2\lambda+1\} \pmod{v}$ is also an orbit of Z_v for each $a \in Z_v$, and $\{a, (2\lambda+1)a\} \equiv \{a, (2\lambda+1)a\} + 2\lambda + 2 \pmod{v}$ if and only if λ is odd and $a = \lambda + 1$ or $3(\lambda+1)$. Thus, the orbits of Z_v, except for $\{\lambda+1, (2\lambda+1)(\lambda+1)\} \equiv \{\lambda+1, 3\lambda+3\} \pmod{v}$ when λ is odd, may be made into pairs so that D includes at most one orbit of each pair:

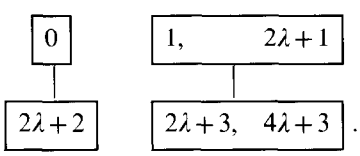
$$\boxed{a, (2\lambda+1)a} \quad \text{—} \quad \boxed{a+2\lambda+2, (2\lambda+1)a+2\lambda+2} \qquad a \in Z_v.$$

The two orbits of each pair are linked by a line, and the pair will be called a line-linked orbit pair, or simply an LL pair.

Table 1

(v, k, λ)	$N(v, k, \lambda)$	Near difference sets
(8, 3, 1)	1	{0, 1, 3}
(12, 5, 2)	1	{0, 1, 2, 5, 10}
(16, 7, 3)	1	{0, 1, 2, 7, 11, 13, 14}
(20, 9, 4)	1	{0, 1, 2, 3, 6, 7, 9, 14, 18}
(24, 11, 5)	1	{0, 1, 2, 8, 11, 15, 16, 17, 19, 21, 22}
(28, 13, 6)	1	{0, 1, 2, 3, 4, 8, 11, 13, 19, 20, 23, 24, 26}
(32, 15, 7)	0	
(36, 17, 8)	1	{0, 1, 2, 4, 5, 7, 10, 11, 12, 13, 17, 21, 24, 26, 32, 33, 34}
(40, 19, 9)	1	{0, 1, 3, 4, 6, 7, 8, 9, 11, 13, 17, 18, 19, 22, 25, 32, 34, 35, 36}
(44, 21, 10)	0	
(48, 23, 11)	1	{0, 1, 2, 3, 4, 5, 8, 9, 10, 15, 18, 19, 21, 23, 30, 31, 35, 37, 38, 40, 41, 44, 46}
(52, 25, 12)	1	{0, 1, 2, 5, 6, 7, 8, 10, 12, 19, 21, 22, 25, 29, 30, 35, 37, 40, 41, 42, 43, 44, 46, 49, 50}
(56, 27, 13)	1	{0, 1, 2, 3, 4, 5, 6, 9, 12, 13, 15, 18, 19, 20, 23, 25, 27, 35, 36, 38, 39, 44, 45, 49, 50, 52, 54}
(60, 29, 14)	$\geqslant 1$	{0, 3, 5, 6, 8, 10, 14, 18, 25, 26, 27, 28, 31, 32, 34, 37, 39, 41, 42, 43, 46, 47, 49, 50, 51, 52, 53, 54, 59}
(64, 31, 15)	$\geqslant 1$	{0, 1, 2, 3, 4, 5, 7, 8, 11, 12, 13, 14, 19, 21, 22, 25, 26, 27, 29, 31, 38, 41, 42, 47, 49, 50, 52, 55, 56, 60, 62}
(68, 33, 16)	0	
(72, 35, 17)	0	

When λ is odd, the orbit $\{\lambda+1, 3\lambda+3\}$ is clearly not included in D. Then D must include exactly one orbit of each LL pair. Consider the following two pairs:



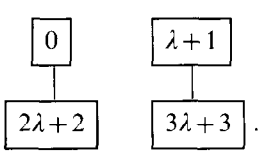
Noting that $(2\lambda+3)\{2\lambda+3, 4\lambda+3\} \equiv \{1, 2\lambda+1\} \pmod{v}$, and that $D, D+2\lambda+3$, $(2\lambda+3)D$ and $(2\lambda+3)(D+2\lambda+2)$ are all fixed by $t=2\lambda+1$, we may assume that

$$\{0\} \cup \{1, 2\lambda+1\} \subseteq D,$$

and then

$$(\{2\lambda+2\} \cup \{\lambda+1, 3\lambda+3\} \cup \{2\lambda+3, 4\lambda+3\}) \cap D = \emptyset.$$

When λ is even, it is easy to see that all the orbits of length one of Z_v are



(6.2)

The other orbits of Z_v are all of length two. As $|D| = 2\lambda+1$ is odd, D must include exactly one of the four orbits in (6.2) and exactly one orbit from each of the other LL

orbit pairs. Since D, $D+2\lambda+2$, $D+\lambda+1$ and $D+3\lambda+3$ are all fixed by $t=2\lambda+1$, we may assume that D contains 0. Furthermore, noting that D includes one of the LL pair $\{1, 2\lambda+1\}$ and $\{2\lambda+3, 4\lambda+3\}$ and that

$$(2\lambda+3)\{2\lambda+3, 4\lambda+3\} \equiv \{1, 2\lambda+1\} \pmod{v},$$

we may also assume that $\{1, 2\lambda+1\}$ is included in D, and then $\{2\lambda+3, 4\lambda+3\}$ must not be included in D.

Summing up, we have the following lemma.

Lemma 6.1. *Let $k=2\lambda+1$ be a prime, D a $(4(\lambda+1), 2\lambda+1, \lambda)$ near difference set, and $kD \equiv D \pmod{v}$. Then we may assume that*

$$\{0, 1, 2\lambda+1\} \subseteq D, \quad \textit{and} \quad \lambda+1, 2\lambda+2, 2\lambda+3, 3\lambda+3 \notin D.$$

Next, we describe some further relations among the orbits of Z_v and introduce some conventions. For an even number d and an orbit $\{a, (2\lambda+1)a\}$ of Z_v, we have

$$\{a+d, (2\lambda+1)a-d\} \equiv (a+d)\{1, 2\lambda+1\} \pmod{v}.$$

So $\{a+d, (2\lambda+1)a-d\}$ is also an orbit of Z_v. Conversely, if there are two orbits $\{a, (2\lambda+1)a\}$ and $\{b, (2\lambda+1)b\}$ with $b-a \equiv d \pmod{v}$, then $\{b, (2\lambda+1)b\} \equiv \{a+d, (2\lambda+1)a-d\}$ as $(2\lambda+1)a-(2\lambda+1)b \equiv -(2\lambda+1)(b-a) \equiv (2\lambda+3)d \equiv d \pmod{v}$. Thus, for any two orbits A, B of Z_v, d either appears exactly two times or does not appear at all in the difference list

$$\{\pm(a-b) \mid a \in A,\ b \in B\}.$$

For a given λ (such that $2\lambda+1$ is a prime) and a given d (even), we now construct a graph G_λ^d with the set

$$\{\{a, (2\lambda+1)a\} \mid a \in Z_v,\ a \not\equiv \lambda+1,\ 2\lambda+2,\ 2\lambda+3 \pmod{v}\} \quad \text{if } 2 \nmid \lambda$$

or

$$\{\{a, (2\lambda+1)a \mid a\} \in Z_v,\ a \not\equiv \lambda+1,\ 2\lambda+2,\ 2\lambda+3,\ 3\lambda+3 \pmod{v}\} \quad \text{if } 2 \mid \lambda$$

as the vertex set, and two orbits $\{a, (2\lambda+1)a\}$, $\{b, (2\lambda+1)b\}$ are linked by a line if they constitute an LL pair, linked by a dotted-line if $\{b, (2\lambda+1)b\} \equiv \{a+d, (2\lambda+1)a-d\} \pmod{v}$, and linked by no line otherwise. The graph G_λ^d is called the characteristic graph of the difference d, and the two orbits are called a dot-linked orbit pair, or simply a DL pair, if they are linked by a dotted line. An LL pair of G is called a distinguished LL pair, or simply a DLL pair, if d appears in the difference list of one orbit of the pair. In this case, d will also appear in the difference list of the other orbit of the pair. As D is a union of some of the orbits in G_λ^d, we may denote by $G_\lambda^d[D]$ the subgraph of G_λ^d induced by the orbits in D. Since D is a near difference set, the number $N(G_\lambda^d[D])$ of DL pairs in $G_\lambda^d[D]$ must be $(\lambda-\delta(d))/2$, where $\delta(d)$ denotes the number of DLL pairs of G_λ^d.

Applying the above observations to the parameters $(8, 3, 1)$ $((12, 5, 2))$, we immediately see that $N(8, 3, 1)=1$ $(N(12, 5, 2)=1)$. We now proceed to deal with the other parameters listed in Table 1.

Lemma 6.2. $N(16,7,3)=1$.

Proof. The graph G_3^2 is given by Fig. 4. There is exactly one DLL pair, which is marked with the symbol '$\cdots 2 \cdots$' above it. (In the sequel, some other similar symbols will be used.) So $N(G_3^2[D])=1$. Thus, D has only two possibilities:

$$D_1=\{0\}\cup\{2,14\}\cup\{1,7\}\cup\{11,13\}=\{0,1,2,7,11,13,14\},$$

$$D_2=\{0\}\cup\{10,6\}\cup\{1,7\}\cup\{3,5\}=\{0,1,3,5,6,7,10\}.$$

It is easily checked that $D_2=3D_1$ and that D_1 is a $(16,7,3)$ near difference set. This completes the proof. □

Lemma 6.3. $N(24,11,5)=1$.

Proof. The orbits of Z_{24} under the permutation $x\to 11x$ are given in Fig. 5.

By Lemma 6.1 we assume that D includes $\{0\}$ and $\{1,11\}$ and thus

$$\{0,1,11\}\subset D \quad \text{and} \quad 12,13,23,6,18\notin D.$$

The characteristic graph G_5^2 and G_5^4 are given in Figs 6 and 7, respectively. There is exactly one DLL pair in each of G_5^2 and G_5^4. Thus

$$N(G_{5,1}^2[D])+N(G_{5,2}^2[D])=N(G_5^2[D])=2=N(G_5^4[D])$$
$$=N(G_{5,1}^4[D])+N(G_{5,3}^4[D]),$$

because $N(G_{5,2}^4[G])=0$. As $N(G_{5,3}^4[G])=0$ or 2, we must have $N(G_{5,1}^4[D])=0$ and hence $N(G_{5,3}^4[D])=2$. Thus, $\{8,16\}\subset D$. Noting that $N(G_{5,1}^2[D])=1$, we have $N(G_{5,2}^2[D])=1$. Therefore, 5 and 7 cannot be contained in D and hence D includes

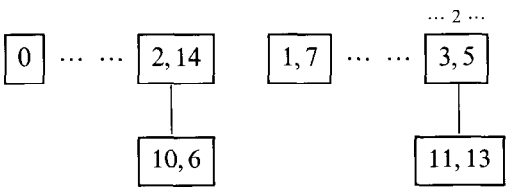
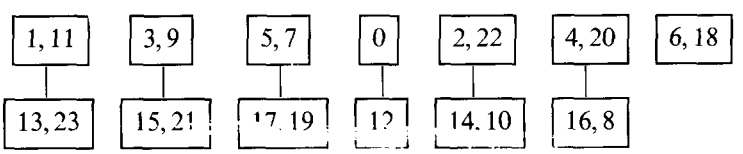


Fig. 4.



(6.3)

Fig. 5

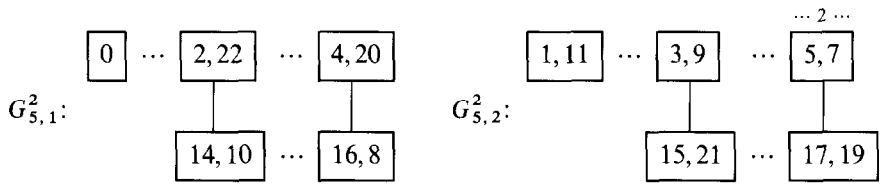


Fig. 6. Graph $G^2_5 = G^2_{5,1} \cup G^2_{5,2}$.

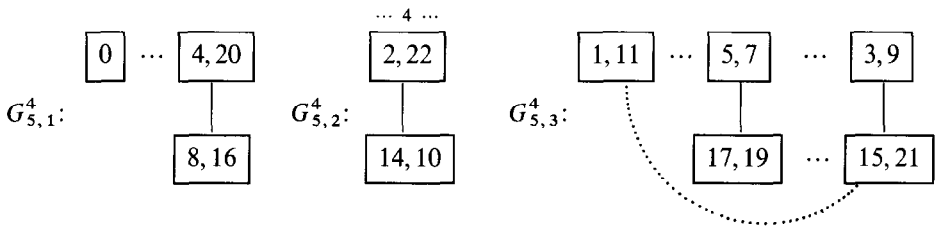


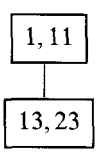
Fig. 7. Graph $G^4_5 = G^4_{5,1} \cup G^4_{5,2} \cup G^4_{5,3}$.

$\{17,19\}$ and $\{15,21\}$ by $N(G^4_{5,3}[D]) = 2$. Consequently, D has only two choices:

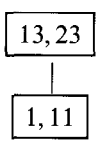
$$D_1 = \{0\} \cup \{8,16\} \cup \{1,11\} \cup \{17,19\} \cup \{15,21\} \cup \{2,22\}$$
$$= \{0,1,2,8,11,15,16,17,19,21,22\},$$
$$D_2 = \{0\} \cup \{8,16\} \cup \{1,11\} \cup \{17,19\} \cup \{15,21\} \cup \{14,10\}$$
$$= \{0,1,8,10,11,14,15,16,17,19,21\}.$$

It is easy to check that $D_2 = 17D_1$ and that D_1 is a $(24,11,5)$ near difference set. This completes the proof. □

Remark. The graphs G^d_λ will play a prominent role in the rest of this paper. For convenience, we sometimes identify their vertices and their LL paris with some letters, numerals and special marks. Fig. 8 expresses that the vertex pair



is identified with a, that 1,11 and 13,23 are identified with $\mathring{a}$ and $\underset{\circ}{a}$, respectively, and that



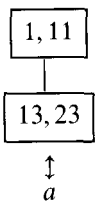


Fig. 8.

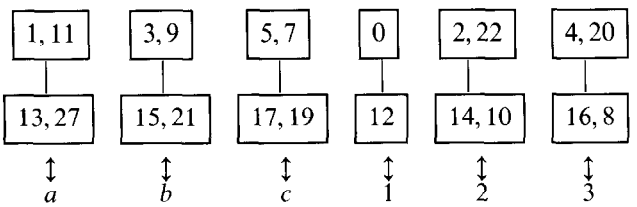


Fig. 9.

is identified with $\bar{a}$. For example, if we identify the LL pairs in (6, 3) in the following way as in Fig. 9, the graphs G_5^2 and G_5^4 may be redrawn as follows:

$$G_5^2 = G_{5,1}^2 \cup G_{5,2}^2, \qquad G_{5,1}^2: \mathring{1}\ 2\ 3, \qquad G_{5,2}^2: \mathring{a}\ b\ c$$

$$G_5^4 = G_{5,1}^4 \cup G_{5,2}^4 \cup G_{5,3}^4, \qquad G_{5,1}^4: \mathring{1}\ 3, \qquad G_{5,2}^4: 2, \qquad G_{5,3}^4: \mathring{a}\ c\ d.$$

The graph $G_{5,1}^4 \cup G_{5,2}^4$ may be redrawn as $\mathring{1}$3-2. To see how these symbols are used, we see two more examples:

(1) In the proof of Lemma 6.5, we have

$$G_8^6 = G_{8,1}^6 \cup G_{8,2}^6 \cup G_{8,3}^6,$$

$$G_{8,1}^6: \mathring{a}\ d\ c \infty b, \qquad G_{8,2}^6: 3\ \bar{5}\ \bar{2}, \qquad G_{8,3}^6: \mathring{1}\ 4$$

with the correspondences (6.6) and (6.7). The original graphs are given in Fig. 10.

(2) In the proof of Lemma 6.6, we have

$$G_9^8 = G_{9,1}^8 \cup G_{9,2}^8, \qquad G_{9,1}^8: \mathring{a}\ e\ b\ \bar{c}\ \bar{d}, \qquad G_{9,2}^8: \mathring{1}\ 5\ \bar{3} \infty 2\ 4$$

with the correspondencde (6.9). The original graphs are given in Fig. 11.

Lemma 6.4. $N(28, 13, 6) = 1$.

Proof. The orbits of Z_{28} under the permutations $x \to 13x$ are given in Fig. 12. □

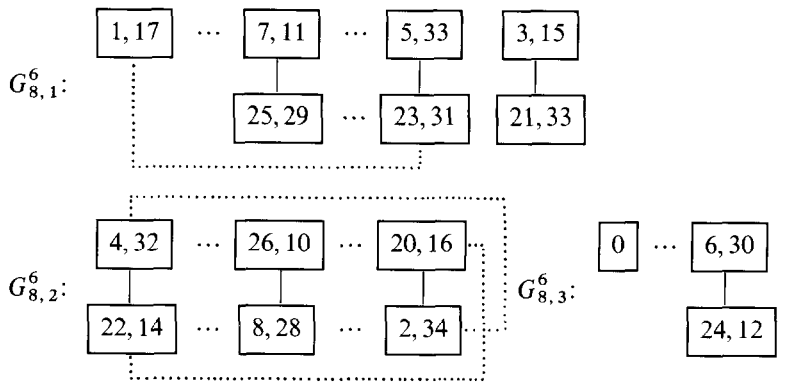


Fig. 10.

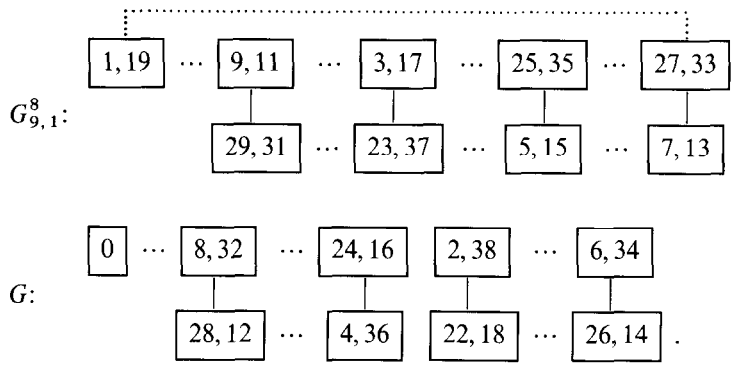


Fig. 11.

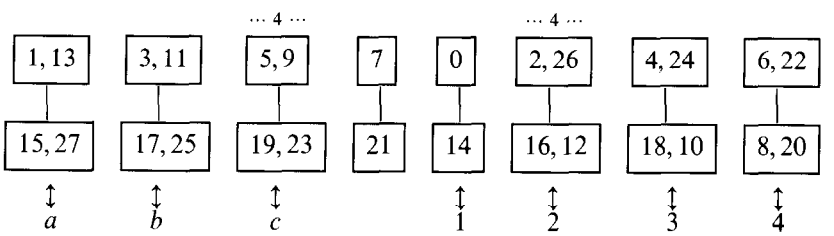


Fig. 12.

By Lemma 6.1 we assume that

$$\{0,1,13\}\subset D, \quad \text{and} \quad 14,7,21,15,27\notin D.$$

The graphs G_6^2 and G_6^4 are

$$G_6^2=G_{6,1}^2\cup G_{6,2}^2, \qquad G_{6,1}^2\colon \mathring{a}\ b\ c, \qquad G_{6,2}^2\colon \mathring{1}\ 2\ 3\ 4,$$
$$G_6^4=G_{6,1}^4\cup G_{6,2}^4, \qquad G\colon b\ \mathring{\bar{a}}\ \bar{c}, \qquad G\colon \mathring{1}\ 3\ \bar{4}\ \bar{2}.$$

Noting that there are two DLL pairs in G_6^4 and no DLL pairs in G_6^2, we have

$$N(G_6^2[D])=N(G_{6,1}^2[D])+N(G_{6,2}^2[D])=3, \tag{6.4}$$

$$N(G_6^4[D])=N(G_{6,1}^4[D])+N(G_{6,2}^4[D])=2. \tag{6.5}$$

In Table 2 we list out all the possible choices of $G_{6,1}^2[D]$ and the corresponding $G_{6,1}^4[D]$ and $N(G_{6,1}^4[D])$. In Table 3, we list out all the choices of $G_{6,2}^2[D]$ and the corresponding $G_{6,2}^4[D]$ and $N(G_{6,2}^4[D])$. The combinations of $G_{6,1}^2[D]$ and $G_{6,2}^2[D]$ must satisfy (6.4) and (6.5). So there are only four choices:

(1) $\mathring{a}\mathring{b}\mathring{c}\cup\mathring{1}\mathring{2}\mathring{3}\mathring{4}$

$$D_1=\{1,13\}\cup\{13,11\}\cup\{5,9\}\cup\{0\}\cup\{16,12\}\cup\{4,24\}\cup\{6,22\}$$
$$=\{0,1,3,4,5,6,9,11,12,13,16,22,24\}.$$

(2) $\mathring{a}\mathring{b}\mathring{c}\cup\mathring{1}\mathring{2}\mathring{3}\mathring{4}$

$$D_2=\{1,13\}\cup\{3,11\}\cup\{5,9\}\cup\{0\}\cup\{16,12\}\cup\{18,10\}\cup\{6,22\}$$
$$=\{0,1,3,5,6,9,10,11,12,13,16,18,22\}.$$

Table 2

$G_{6,1}^2[D]$	$N(G_{6,1}^2[D])$	$G_{6,1}^4[D]$	$N(G_{6,1}^4[D])$
$\mathring{a}\mathring{b}\mathring{c}$	2	$\mathring{b}\bar{\mathring{a}}\bar{\mathring{c}}$	1
$\mathring{a}\mathring{b}\mathring{c}$	1	$\mathring{b}\bar{\mathring{a}}\mathring{c}$	0
$\mathring{a}\mathring{b}\mathring{c}$	0	$b\bar{\mathring{a}}\bar{\mathring{c}}$	2
$\mathring{a}\mathring{b}\mathring{c}$	1	$b\bar{\mathring{a}}\mathring{c}$	1

Table 3

$G_{6,2}^2[D]$	$N(G_{6,2}^2[D])$	$G_{6,2}^4[D]$	$N(G_{6,2}^4[D])$
$\mathring{1}\mathring{2}\mathring{3}\mathring{4}$	3	$\mathring{1}\mathring{3}\bar{\mathring{4}}\bar{\mathring{2}}$	2
$\mathring{1}\mathring{2}\mathring{3}\mathring{4}$	2	$\mathring{1}\mathring{3}\mathring{4}\bar{\mathring{2}}$	2
$\mathring{1}\mathring{2}\mathring{3}\mathring{4}$	1	$\mathring{1}3\bar{\mathring{4}}\bar{\mathring{2}}$	2
$\mathring{1}\mathring{3}\mathring{3}4$	2	$\mathring{1}3\mathring{4}\bar{\mathring{2}}$	0
$\mathring{1}\mathring{2}\mathring{3}\mathring{4}$	1	$\mathring{1}\mathring{3}\bar{\mathring{4}}\mathring{2}$	1
$\mathring{1}\mathring{2}\mathring{3}\mathring{4}$	0	$\mathring{1}\mathring{3}\mathring{4}\mathring{2}$	3
$\mathring{1}\mathring{2}\mathring{3}\mathring{4}$	1	$\mathring{1}3\bar{\mathring{4}}\mathring{2}$	1
$\mathring{1}234$	2	$\mathring{1}3\mathring{4}\mathring{2}$	1

(3) $\mathring{a}\mathring{b}\mathring{c}\cup\mathring{1}\mathring{2}\mathring{3}\mathring{4}$

$$D_3=\{1,13\}\cup\{3,11\}\cup\{19,23\}\cup\{0\}\cup\{2,26\}\cup\{4,24\}\cup\{8,20\}$$
$$=\{0,1,2,3,4,8,9,11,13,19,20,23,24,26\}.$$

(4) $\mathring{a}\mathring{b}\mathring{c}\cup\mathring{1}\mathring{2}\mathring{3}\mathring{4}$

$$D_4=\{1,13\}\cup\{17,25\}\cup\{19,23\}\cup\{0\}\cup\{16,12\}\cup\{18,10\}\cup\{8,20\}$$
$$=\{0,1,8,10,12,13,16,17,18,19,20,23,25\}.$$

It is easy to check that

$$D_1=11D_3,\qquad D_4=19D_3,$$

that D_3 is a (28, 13, 6) near difference set and that D_2 is not (as 6 appears eight times in the difference list of D). This completes the proof. □

Lemma 6.5. $N(36,17,8)=1$.

Proof. Under the permutation $x\to 17x$, Z_{36} is partitioned into orbits as given in Fig. 13.

By Lemma 6.1, we assume that

$$\{0,1,17\}\subset D,\qquad 18,19,35,9,27\notin D$$

The graphs G_8^w $(w=2,4,6,8)$ are

$G_8^2=G_{8,1}^2\cup G_{8,2}^2$ with

$G_{8,1}^2$: $\mathring{a}bcd$, $G_{8,2}^2$: $\mathring{1}2345$

$G_8^4=G_{8,1}^4\cup G_{8,2}^4$: with

$G_{8,1}^4$: $c\mathring{a}\bar{b}\bar{d}$, $G_{8,2}^4$: $\mathring{1}35\bar{4}\bar{2}$.

$G_8^6=G_{8,1}^6\cup G_{8,2}^6\cup G_{8,3}^6$: with

$G_{8,1}^6$: $\mathring{a}dc\infty b$, $G_{8,2}^6$: $3\bar{5}\bar{2}$ $G_{8,3}^6=\mathring{1}4$,

$G_8^8=G_{8,1}^8\cup G_{8,2}^8$ with

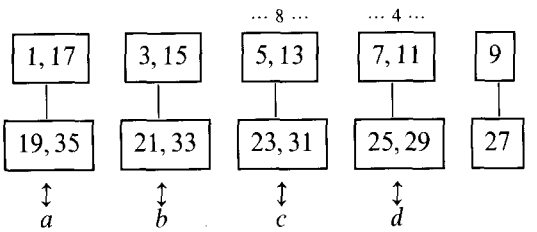
$G_{8,1}^8$: $\mathring{a}\bar{d}\bar{b}c$, $G_{8,2}^8$: $\mathring{1}5\bar{2}\bar{4}3$.

Noting that there are two DLL pairs in each of G_8^4 and G_8^8, i.e. d and 2 in G_8^4, c and 3 in G_8^8, we have

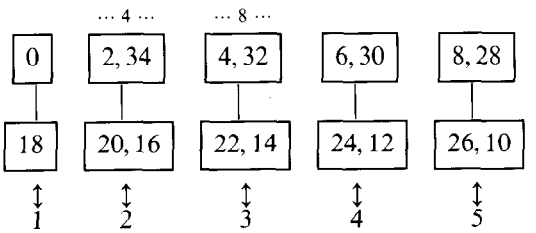
$$N(G_{8,1}^w[D])+N(G_{8,2}^w[D])=N(G_8^w[D])=\begin{cases}3, & w=4,8\\ 4, & w=2,6.\end{cases}\tag{6.8}$$

Consider the graph G_8^6. Noting that D contains exactly one orbit of each LL pair, we have

$$N(G_{8,1}^6[D])=0,\text{ or }2;\qquad N(G_{8,2}^6[D])=0,\text{ or }2;\qquad N(G_{8,3}^6[D])=0,\text{ or }1.$$



(6.6)



(6.7)

Fig. 13.

As their sum $N(G_8^6[D])$ must be 4 by (6.8), we have

$$N(G_{8,3}^6[D])=0 \quad \text{and} \quad N(G_{8,1}^6[D])=N(G_{8,2}^6[D])=2.$$

Hence

$$\underset{\circ}{4}=\{24,12\}\subset D.$$

In Tables 4 and 5, we list out all the possible choices of $G_{8,i}^6[D]$ such that $N(G_{8,i}^6[D])=2$ and the corresponding $G_{8i}^w[D]$ and $N(G_{8,i}^w[D])(w=2,4,8)$ for $i=1$ and 2, respectively. The combinations of $G_{8,1}^6[D]$ and $G_{8,2}^6[D]$ must satisfy (6.8), so D has only three possible choices:

(1) $\mathring{a}\mathring{d}\mathring{c}\infty\underset{\circ}{b}$ and $\mathring{\bar{3}}\mathring{\bar{5}}\underset{\circ}{\bar{2}}$

$$D_1=\{1,17\}\cup\{7,11\}\cup\{5,13\}\cup\{21,33\}\cup\{0\}\cup\{24,12\}\cup\{4,32\}$$
$$\cup\{26,10\}\cup\{2,34\}$$
$$=\{0,1,2,4,5,7,10,11,12,13,17,21,24,26,32,33,34\}.$$

(2) $\mathring{a}\mathring{d}\underset{\circ}{c}\infty\mathring{b}$ and $\underset{\circ}{\mathring{3}}\mathring{\bar{5}}\mathring{\bar{2}}$

$$D_2=\{1,17\}\cup\{7,11\}\cup\{23,31\}\cup\{3,15\}\cup\{0\}\cup\{24,12\}\cup\{22,14\}$$
$$\cup\{26,10\}\cup\{20,16\}.$$
$$=\{0,1,3,7,10,11,12,14,15,16,17,20,22,23,24,26,31\}.$$

(3) $\mathring{a}\underset{\circ}{\mathring{d}}\underset{\circ}{c}\infty\underset{\circ}{b}$ and $\underset{\circ}{3}\underset{\circ}{\bar{5}}\underset{\circ}{\bar{2}}$

$$D_3=\{1,17\}\cup\{25,29\}\cup\{23,31\}\cup\{21,33\}\cup\{0\}\cup\{24,12\}\cup\{22,14\}$$
$$\cup\{8,28\}\cup\{2,34\}.$$
$$=\{0,1,2,8,12,14,17,21,22,23,24,25,28,29,31,33,34\}.$$

Table 4

$G^6_{8,1}[D]$	$G^2_{8,1}[D]$,	$N(G^2_{8,1}[D])$	$G^4_{8,1}[D]$,	$N(G^4_{8,1}[D])$	$G^8_{8,1}[D]$,	$N(G^8_{8,1}[D])$
$\overset{\circ}{a}\overset{\circ}{d}\overset{\circ}{c}\infty\overset{\circ}{b}$	$\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{c}\overset{\circ}{d}$	3	$\overset{\circ}{c}\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{d}$	2	$\overset{\circ}{a}\overset{\circ}{d}\overset{\circ}{b}\overset{\circ}{c}$	1
$\overset{\circ}{a}\overset{\circ}{d}\overset{\circ}{c}\infty\overset{\circ}{b}$	$\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{c}\overset{\circ}{d}$	1	$\overset{\circ}{c}\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{d}$	2	$\overset{\circ}{a}\overset{\circ}{d}\overset{\circ}{b}\overset{\circ}{c}$	1
$\overset{\circ}{a}\overset{\circ}{d}\overset{\circ}{c}\infty\overset{\circ}{b}$	$\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{c}\overset{\circ}{d}$	1	$\overset{\circ}{c}\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{d}$	1	$\overset{\circ}{a}\overset{\circ}{d}\overset{\circ}{b}\overset{\circ}{c}$	2
$\overset{\circ}{a}\overset{\circ}{d}\overset{\circ}{c}\infty\overset{\circ}{b}$	$\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{c}\overset{\circ}{d}$	1	$\overset{\circ}{c}\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{d}$	1	$\overset{\circ}{a}\overset{\circ}{d}\overset{\circ}{b}\overset{\circ}{c}$	0
$\overset{\circ}{a}\overset{\circ}{d}\overset{\circ}{c}\infty\overset{\circ}{b}$	$\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{c}\overset{\circ}{d}$	2	$\overset{\circ}{c}\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{d}$	0	$\overset{\circ}{a}\overset{\circ}{d}\overset{\circ}{b}\overset{\circ}{c}$	2
$\overset{\circ}{a}\overset{\circ}{d}\overset{\circ}{c}\infty\overset{\circ}{b}$	$\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{c}\overset{\circ}{d}$	2	$\overset{\circ}{c}\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{d}$	2	$\overset{\circ}{a}\overset{\circ}{d}\overset{\circ}{b}\overset{\circ}{c}$	2

Table 5

$G^6_{8,2}[D]$	$G^2_{8,2}[D]$,	$N(G^2_{8,2}[D])$	$G^4_{8,2}[D]$,	$N(G^2_{8,4}[D])$	$G^8_{8,2}[D]$,	$N(G^8_{8,2}[D])$
$\overset{\circ}{3}\overset{\circ}{5}\overset{\circ}{2}$	$\overset{\circ}{1}\overset{\circ}{2}\overset{\circ}{3}45$	1	$\overset{\circ}{1}\overset{\circ}{3}\overset{\circ}{5}\overset{\circ}{4}\overset{\circ}{2}$	2	$\overset{\circ}{1}\overset{\circ}{5}\overset{\circ}{2}\overset{\circ}{4}\overset{\circ}{3}$	2
$\overset{\circ}{3}\overset{\circ}{5}\overset{\circ}{2}$	$\overset{\circ}{1}\overset{\circ}{2}\overset{\circ}{3}45$	3	$\overset{\circ}{1}\overset{\circ}{3}\overset{\circ}{5}\overset{\circ}{4}\overset{\circ}{2}$	1	$\overset{\circ}{1}\overset{\circ}{5}\overset{\circ}{2}\overset{\circ}{4}\overset{\circ}{3}$	2
$\overset{\circ}{3}\overset{\circ}{5}\overset{\circ}{2}$	$\overset{\circ}{1}\overset{\circ}{2}\overset{\circ}{3}\overset{\circ}{4}5$	2	$\overset{\circ}{1}\overset{\circ}{3}\overset{\circ}{5}\overset{\circ}{4}\overset{\circ}{2}$	3	$\overset{\circ}{1}\overset{\circ}{5}\overset{\circ}{2}\overset{\circ}{4}3$	2
$\overset{\circ}{3}\overset{\circ}{5}\overset{\circ}{2}$	$\overset{\circ}{1}2345$	3	$\overset{\circ}{1}3\overset{\circ}{5}\overset{\circ}{4}\overset{\circ}{2}$	2	$\overset{\circ}{1}\overset{\circ}{5}\overset{\circ}{2}\overset{\circ}{4}3$	1
$\overset{\circ}{3}\overset{\circ}{5}\overset{\circ}{2}$	$\overset{\circ}{1}2345$	2	$\overset{\circ}{1}3\overset{\circ}{5}\overset{\circ}{4}\overset{\circ}{2}$	2	$\overset{\circ}{1}\overset{\circ}{5}\overset{\circ}{2}\overset{\circ}{4}3$	3
$\overset{\circ}{3}\overset{\circ}{5}\overset{\circ}{2}$	$\overset{\circ}{1}2345$	2	$\overset{\circ}{1}3\overset{\circ}{5}\overset{\circ}{4}\overset{\circ}{2}$	1	$\overset{\circ}{1}\overset{\circ}{5}\overset{\circ}{2}\overset{\circ}{4}3$	1

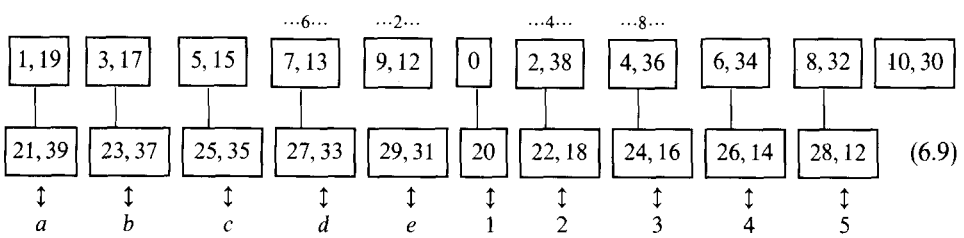
It is easy to check that

$$D_2 = -5D_1, \qquad D_3 = -7D_1,$$

and that D_1 is a $(36, 17, 8)$ near difference set. This completes the proof. □

Lemma 6.6. $N(40, 19, 9) = 1$.

Proof. The orbits of Z_{40} under the permutation $x \to 19x$ are:



(6.9)

By Lemma 6.1 we assume that

$$\{0, 1, 19\} \subset D, \qquad 20, 21, 39, 10, 30 \notin D$$

The graphs G_9^w ($w = 2, 4, 6, 8$) are:

$G_9^2 = G_{9,1}^2 \cup G_{9,2}^2$: $\qquad G_9^4 = G_{9,1}^4 \cup G_{9,2}^4$:

$G_{9,1}^2$: $\mathring{a}bcde$, $\qquad G$: 12345 $\qquad G_{9,1}^4$: $\mathring{a}cedb$, $\qquad G_{9,2}^4$: $\mathring{1}35\infty24$

$G_9^6 = G_{9,1}^6 \cup G_{9,2}^6$: $\qquad G_9^8 = G_{9,1}^8 \cup G_{9,2}^8$:

$G_{9,1}^6$: $bec\mathring{\bar{a}}\bar{d}$, $\qquad G_{9,2}^6$: $14\bar{5}\bar{2}\bar{3}$ $\qquad G_{9,1}^8$: $\mathring{a}eb\bar{c}\bar{d}$, $\qquad G_{9,2}^8$: $\mathring{1}5\bar{3}\infty24$

It is easy to see that there is exactly one DLL pair in each of G_9^w, $w = 2, 4, 6, 8$, so

$$N(G_9^w[D]) = N(G_{9,1}^w[D]) + N(G_{9,2}^w[D]) = 4, \quad \text{for } w = 2, 4, 6, 8. \tag{6.10}$$

Noting that $N(G_{9,1}^4[D]) = 0, 2$, or 4 $N(G_{9,2}^4[D]) = 0, 1, 2$, or 3, we have

$$N(G_{9,1}^4[D]) = 4 \quad \text{and} \quad N(G_{9,2}^4[D]) = 0 \tag{6.11}$$

or

$$N(G_{9,1}^4[D]) = 2 \quad \text{and} \quad N(G_{9,2}^4[D]) = 2. \tag{6.12}$$

Similarly, noting that $N(G_{9,1}^8[D]) = 1, 3$, or 5 and $N(G_{9,2}^8[D]) = 0, 1, 2$, or 3, we have

$$N(G_{9,1}^8[D]) = 1 \quad \text{and} \quad N(G_{9,2}^8[D]) = 3 \tag{6.13}$$

or

$$N(G_{9,1}^8[D]) = 3 \quad \text{and} \quad N(G_{9,2}^8[D]) = 1 \tag{6.14}$$

(6.11) and (6.13) are impossible, for $N(G_{9,2}^4[D]) = 0$ implies $N(G_{9,2}^8[D]) = 2$, and for $N(G_{9,2}^8[D]) = 3$ implies $N(G_{9,2}^4[D]) = 1$.

Tables 6 and 7 list out all the possible $G_{9,1}^8[D]$ and $G_{9,2}^8[D]$, respectively, and when (6.12) is satisfied we also list the corresponding $G_{9,i}^w[D]$ and $N(G_{9,i}^w[D])$ for $w = 2, 6$, $i = 1, 2$. The combinations of $G_{9,1}^8[D]$ and $G_{9,2}^8[D]$ must satisfy (6.10), so D has only four possible choices:

(1) $\mathring{a}\mathring{e}\mathring{b}\mathring{\bar{c}}\mathring{\bar{d}}$ and $\mathring{1}\mathring{5}\mathring{\bar{3}}\mathring{\infty}\mathring{2}\mathring{4}$

$$D_1 = \{1, 19, 9, 11, 3, 17, 25, 35, 7, 13, 0, 8, 32, 4, 36, 22, 18, 6, 34\}$$
$$= \{0, 1, 3, 4, 6, 7, 8, 9, 11, 13, 17, 18, 19, 22, 25, 32, 34, 35, 36\},$$

(2) $\mathring{a}\mathring{e}b\mathring{\bar{c}}\mathring{\bar{d}}$ and $\mathring{1}\mathring{5}\mathring{\bar{3}}\mathring{\infty}\mathring{2}\mathring{4}$

$$D_2 = \{1, 19, 9, 11, 23, 37, 25, 35, 27, 33, 0, 8, 32, 4, 36, 2, 38, 26, 14\}$$
$$= \{0, 1, 2, 4, 8, 9, 11, 14, 19, 23, 25, 26, 27, 32, 33, 35, 36, 37, 38\}.$$

(3) $\mathring{a}\mathring{e}\mathring{b}\mathring{\bar{c}}\mathring{\bar{d}}$ and $\mathring{1}\mathring{5}\mathring{\bar{3}}\mathring{\infty}\mathring{2}\mathring{4}$

$$D_3\{1, 19, 29, 31, 3, 17, 25, 35, 27, 33, 0, 28, 12, 24, 16, 2, 38, 6, 34\}$$
$$= \{0, 1, 2, 3, 6, 12, 16, 17, 19, 24, 25, 27, 28, 29, 31, 33, 34, 35, 38\}.$$

Table 6

$G^8_{9,1}[D]$	$G^4_{9,1}[D]$,	$N(G^4_{9,1}[D])$	$G^2_{9,1}[D]$,	$N(G^2_{9,1}[D])$	$G^6_{9,1}[D]$,	$N(G^4_{9,1}[D])$
$\overset{\circ}{a}\overset{\circ}{e}\overset{\circ}{b}\overset{\circ}{\bar{c}}\overset{\circ}{\bar{d}}$	$\overset{\circ}{a}\underset{\circ}{c}\overset{\circ}{e}\overset{\circ}{d}\underset{\circ}{b}$	2	$\overset{\circ}{a}\overset{\circ}{b}\underset{\circ}{c}\overset{\circ}{d}\overset{\circ}{e}$	2	$\overset{\circ}{b}\overset{\circ}{e}\underset{\circ}{c}\overset{\circ}{\bar{a}}\overset{\circ}{\bar{d}}$	3
$\overset{\circ}{a}\overset{\circ}{e}\overset{\circ}{b}\underset{\circ}{\bar{c}}\overset{\circ}{\bar{d}}$	$\overset{\circ}{a}\overset{\circ}{c}\overset{\circ}{e}\underset{\circ}{d}\overset{\circ}{b}$	2	$\overset{\circ}{a}\overset{\circ}{b}\overset{\circ}{c}\underset{\circ}{d}\overset{\circ}{e}$	2	$\overset{\circ}{b}\overset{\circ}{e}\overset{\circ}{c}\underset{\circ}{\bar{a}}\overset{\circ}{\bar{d}}$	2
$\overset{\circ}{a}\overset{\circ}{e}\overset{\circ}{b}\underset{\circ}{\bar{c}}\underset{\circ}{\bar{d}}$	$\overset{\circ}{a}\overset{\circ}{c}\overset{\circ}{e}\overset{\circ}{d}\overset{\circ}{b}$	4				
$\overset{\circ}{a}\overset{\circ}{e}\underset{\circ}{b}\overset{\circ}{\bar{c}}\overset{\circ}{\bar{d}}$	$\overset{\circ}{a}\underset{\circ}{c}\overset{\circ}{e}\underset{\circ}{d}\overset{\circ}{b}$	2	$\overset{\circ}{a}\underset{\circ}{b}\underset{\circ}{c}\overset{\circ}{d}\overset{\circ}{e}$	2	$\overset{\circ}{b}\underset{\circ}{e}\overset{\circ}{c}\overset{\circ}{\bar{a}}\overset{\circ}{\bar{d}}$	1
$\overset{\circ}{a}\overset{\circ}{e}\underset{\circ}{b}\overset{\circ}{\bar{c}}\overset{\circ}{\bar{d}}$	$\overset{\circ}{a}\overset{\circ}{c}\overset{\circ}{e}\overset{\circ}{d}\underset{\circ}{b}$	4				
$\overset{\circ}{a}\overset{\circ}{e}\underset{\circ}{b}\underset{\circ}{\bar{c}}\overset{\circ}{\bar{d}}$	$\overset{\circ}{a}\overset{\circ}{c}\overset{\circ}{e}\overset{\circ}{d}\overset{\circ}{b}$	4				
$\overset{\circ}{a}\underset{\circ}{e}\overset{\circ}{b}\overset{\circ}{\bar{c}}\overset{\circ}{\bar{d}}$	$\overset{\circ}{a}\underset{\circ}{c}\overset{\circ}{e}\underset{\circ}{d}\overset{\circ}{b}$	2	$\overset{\circ}{a}\overset{\circ}{b}\underset{\circ}{c}\underset{\circ}{d}\overset{\circ}{e}$	3	$\overset{\circ}{b}\underset{\circ}{e}\overset{\circ}{c}\overset{\circ}{\bar{a}}\overset{\circ}{\bar{d}}$	2
$\overset{\circ}{a}\underset{\circ}{e}\overset{\circ}{b}\underset{\circ}{\bar{c}}\overset{\circ}{\bar{d}}$	$\overset{\circ}{a}\underset{\circ}{c}\underset{\circ}{e}\underset{\circ}{d}\overset{\circ}{b}$	4				
$\overset{\circ}{a}\underset{\circ}{e}\overset{\circ}{b}\underset{\circ}{\bar{c}}\overset{\circ}{\bar{d}}$	$\overset{\circ}{a}\overset{\circ}{c}\underset{\circ}{e}\underset{\circ}{d}\overset{\circ}{b}$	4				
$\overset{\circ}{a}\underset{\circ}{e}\underset{\circ}{b}\overset{\circ}{\bar{c}}\overset{\circ}{\bar{d}}$	$\overset{\circ}{a}\underset{\circ}{c}\overset{\circ}{e}\underset{\circ}{d}\underset{\circ}{b}$	2	$\overset{\circ}{a}\underset{\circ}{b}\overset{\circ}{c}\underset{\circ}{d}\underset{\circ}{e}$	1	$\underset{\circ}{b}\underset{\circ}{e}\overset{\circ}{c}\overset{\circ}{\bar{a}}\overset{\circ}{\bar{d}}$	2

Table 7

$G^8_{9,2}[D]$	$G^4_{9,2}[D]$,	$N(G^4_{9,2}[D])$	$G^2_{9,2}[D]$,	$N(G^2_{9,2}[D])$	$G^6_{9,2}[D]$,	$N(G^4_{9,2}[D])$
$\overset{\circ}{1}\overset{\circ}{5}\underset{\circ}{\bar{3}}\infty\underset{\circ}{2}\overset{\circ}{4}$	$\overset{\circ}{1}\overset{\circ}{3}\overset{\circ}{5}\infty\underset{\circ}{2}\overset{\circ}{4}$	2	$\overset{\circ}{1}\overset{\circ}{2}\overset{\circ}{3}\overset{\circ}{4}\underset{\circ}{5}$	2	$\overset{\circ}{1}\overset{\circ}{4}\underset{\circ}{\bar{5}}\underset{\circ}{2}\underset{\circ}{\bar{3}}$	3
$\overset{\circ}{1}\overset{\circ}{5}\underset{\circ}{\bar{3}}\infty\underset{\circ}{2}\overset{\circ}{4}$	$\overset{\circ}{1}\overset{\circ}{3}\overset{\circ}{5}\infty\underset{\circ}{2}\overset{\circ}{4}$	2	$\overset{\circ}{1}\underset{\circ}{2}\overset{\circ}{3}\overset{\circ}{4}\underset{\circ}{5}$	2	$\overset{\circ}{1}\overset{\circ}{4}\underset{\circ}{5}\underset{\circ}{2}\underset{\circ}{\bar{3}}$	1
$\overset{\circ}{1}\underset{\circ}{5}\underset{\circ}{\bar{3}}\infty\underset{\circ}{2}\overset{\circ}{4}$	$\overset{\circ}{1}\overset{\circ}{3}\underset{\circ}{5}\infty\underset{\circ}{2}\overset{\circ}{4}$	1				
$\overset{\circ}{1}\underset{\circ}{5}\underset{\circ}{\bar{3}}\infty\underset{\circ}{2}\overset{\circ}{4}$	$\overset{\circ}{1}\overset{\circ}{3}\underset{\circ}{5}\infty\underset{\circ}{2}\overset{\circ}{4}$	1				
$\overset{\circ}{1}\underset{\circ}{5}\overset{\circ}{\bar{3}}\infty\overset{\circ}{2}\overset{\circ}{4}$	$\overset{\circ}{1}\underset{\circ}{3}\underset{\circ}{5}\infty\overset{\circ}{2}\overset{\circ}{4}$	2	$\overset{\circ}{1}\overset{\circ}{2}\overset{\circ}{3}\underset{\circ}{4}\underset{\circ}{5}$	1	$\overset{\circ}{1}\overset{\circ}{4}\overset{\circ}{\bar{5}}\overset{\circ}{2}\overset{\circ}{\bar{3}}$	2
$\overset{\circ}{1}\underset{\circ}{5}\overset{\circ}{\bar{3}}\infty\underset{\circ}{2}\underset{\circ}{4}$	$\overset{\circ}{1}\underset{\circ}{3}\underset{\circ}{5}\infty\underset{\circ}{2}\underset{\circ}{4}$	2	$\overset{\circ}{1}\underset{\circ}{2}\underset{\circ}{3}\underset{\circ}{4}\underset{\circ}{5}$	3	$\overset{\circ}{1}\underset{\circ}{4}\overset{\circ}{\bar{5}}\overset{\circ}{2}\overset{\circ}{\bar{3}}$	2

(4) $\overset{\circ}{a}\underset{\circ}{e}\overset{\circ}{b}\underset{\circ}{\bar{c}}\underset{\circ}{\bar{d}}$ and $\overset{\circ}{1}\underset{\circ}{5}\overset{\circ}{\bar{3}}\infty\underset{\circ}{2}\underset{\circ}{4}$

$$D_4=\{1,19,29,31,23,37,5,15,7,13,0,28,12,24,16,22,13,26,14\}$$

$$=\{0,1,5,7,12,13,14,15,16,18,19,22,23,24,26,28,29,31,37\}.$$

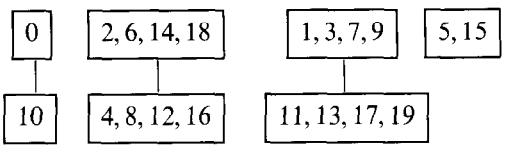
It can be checked that

$$D_2=11D_1,\qquad D_3=-7D_1,\quad D_4=-3D_1,$$

and that D is a $(40,19,9)$ near difference set. This completes the proof. □

Lemma 6.7. $N(20,9,4)=1$.

Proof. Suppose D is a $(20,9,4)$ near difference set. By Theorem 2.1, 3 is a multiplier of D and we mady assume that 3 fixed D. The orbits of Z_{20} under the permutation $x\to 3x$ are



Evidently, D cannot include $\{5,15\}$. Since $D, D+10, 11D$ and $11(D+10)$ are all fixed by 3 and 11 $\{11,13,17,19\}=\{1,3,7,9\}$, we may assume that

$$\{0,1,3,7,9\}\subset D$$

If $\{4,8,12,16\}\subset D$, then D would produce 4 as a difference at least five times, contradicting $\lambda=4$. Therefore

$$D=\{0\}\cup\{1,3,7,9\}\cup\{2,6,14,18\}=\{0,1,2,3,6,7,9,14,18\}.$$

It can be checked that D is indeed a $(20,9,4)$ near difference set. This completes the proof. □

Lemma 6.8. $N(32,15,7)=0$.

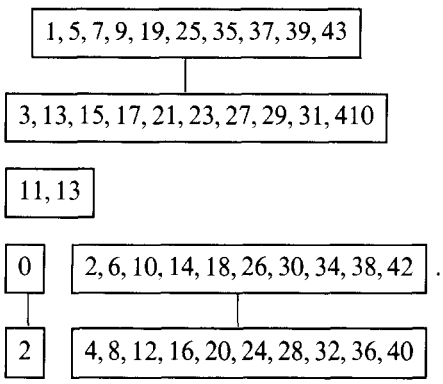
Proof. Suppose that D is a $(32,15,7)$ near difference set in Z_{32}. Since $3^6\equiv 25\equiv 5^2 \pmod{32}$, 25 is a multiplier of D by Theorem 2.1, and we may assume that 25 fixes D. As $25^2\equiv 17 \pmod{32}$, $17a$ is also in D when $a\in D$. Since

$$17a-a=16a\equiv\begin{cases}0 \pmod{32}, & \text{if } 2a,\\ 16 \pmod{32}, & \text{if } 2\not| a,\end{cases}$$

it follows that D contains only even numbers in Z_{32}. Then any odd number in Z_{32} cannot appear in the difference list of D. Hence D is not a $(32,15,17)$ near difference set. This completes the proof. □

Lemma 6.9. $N(44,21,10)=0$.

Proof. Suppose that D is a $(44,21,10)$ near difference set in Z_{44}. Since $3^{12}\equiv 7 \pmod{44}$, 7 is a multiplier of D by Theorem 2.1, and we may assume that 7 fixes D. The orbits of Z_{44} under the permutation $x\to 7x$ are



(6.15)

(6.16)

(6.17)

Clearly, D cannot include $\{11, 33\}$. As D, $29D$, $D+22$ and $29D+22$ are all fixed by 7 and

$$29\{3, 13, 15, 17, 21, 23, 27, 29, 31, 41\}$$
$$\equiv \{1, 5, 7, 9, 19, 25, 35, 37, 39, 43\} \pmod{44}$$

we may assume that

$$D \supset \{0, 1, 5, 7, 9, 19, 25, 35, 37, 39, 43\}.$$

It is easy to check that no matter which orbit of the second pair in (6.17) is included in D, 2 appears in the difference list of D at most seven times, contradicting $\lambda = 10$. This completes the proof. □

Lemma 6.10. $N(48, 23, 11) = 1$.

Proof. The proof is similar to that of Lemmas 6.5 and 6.6, hence is omitted. □

Lemma 6.11. $N(52, 25, 12) = 1$.

Proof. Let D be a $(52, 25, 12)$ near difference set. By Theorem 2.1, 5 is a multiplier of D, and we may assume that D is fixed by 5. Then D will be a union of some of the orbits of Z_{52} under the permutation $x \to 5x$:

$$\begin{array}{llll} a = \{1, 5, 21, 25\} & b = \{3, 11, 15, 23\} & c = \{7, 19, 35, 43\} & \{13\} \\ | & | & | & | \\ a' = \{27, 31, 47, 51\} & b' = \{29, 37, 41, 49\} & c' = \{9, 17, 33, 45\} & \{39\} \end{array}$$

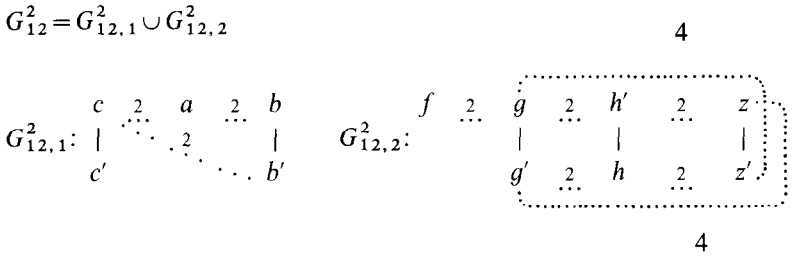
$$\begin{array}{llll} f = \{0\} & g = \{2, 10, 42, 50\} & h = \{6, 22, 30, 46\} & z = \{14, 18, 34, 38\} \\ | & | & | & | \\ f' = \{26\} & g' = \{28, 36, 16, 24\} & h' = \{4, 20, 32, 48\} & z' = \{8, 12, 40, 44\} \end{array}$$

As $D+26$, $27D$, $27D+26$ are all fixed by 5 and $27a' = a$, we may assume that

$$\{0, 1, 5, 21, 25\} \subset D \quad \text{and} \quad 27, 31, 47, 51, 26, 13, 39 \notin D.$$

We construct the characteristic graph of the difference 2 as follows:

$$G_{12}^2 = G_{12,1}^2 \cup G_{12,2}^2$$



This is a weighted graph, and the symbol '$w \overset{m}{\cdots} z$' means that the number of occurrences of 2 in the difference list $\{\pm(x-y) \mid x \in w,\ y \in z\}$ is m. Similarly, we construct the characteristic graph of the difference 8 as in Fig. 14.

$$G_{12}^8 = G_{12,1}^8 \cup G_{12,2}^8$$

Let $N'(G[D])$ be the sum of the numbers on dotted-lines in the graph $G[D]$. Noting that 2 cannot appear in the difference list of any orbit, we have

$$N'(G_{12}^2[D]) = N'(G_{12,1}^2[D]) + N'(G_{12,2}^2[D]) = 12. \tag{6.18}$$

For each orbit, we find the number of occurrences of 8 in its difference list:

a: 0, b (or b'): 2, c (or c'): 1

f: 0, g (or g'): 2, h (or h'): 1, z (or z'): 0.

Hence, we have

$$N'(G_{12}^8[D]) = N'(G_{12,1}^8[D]) + N(G_{12,2}^8[D]) = 6 \tag{6.19}$$

By (6.18) and (6.19) it is known that D has only two possibilities:

(1) $D_1 = a \cup c \cup b \cup f \cup z \cup g \cup h$

$= \{0, 1, 2, 5, 6, 7, 8, 10, 12; 19, 21, 22, 25, 29, 30, 35, 37$

$40, 41, 42, 43, 44, 46, 49, 50\}$,

(2) $D_2 = a \cup b \cup c \cup f \cup z \cup g \cup h$

$= \{0, 1, 3, 5, 6, 7, 11, 14, 15, 16, 18, 19, 21, 22, 23, 24, 25, 28, 30, 34,$

$35, 36, 38, 43, 46\}$.

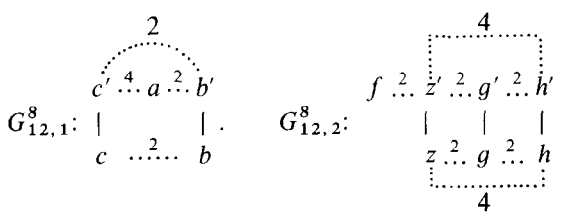


Fig. 14.

It is easy to check that $D_2 = 3D_1$ and that D_1 is a (52, 25, 12) near difference set. This completes the proof. □

Lemma 6.12. $N(56, 27, 13) = 1$.

Proof. Let D be a (56, 27, 13) near difference set. By Theorem 2.1, 3 is a multiplier of D, and we may assume that D is fixed by 3. Then D is a union of some of the orbits of Z_{56} under the permulation $x \to 3x$:

$$\begin{array}{lll} a=\{1,3,9,19,25,27\} & b=\{5,13,15,23,39,45\} & c=\{7,21\} \\ | & | & | \\ a'=\{29,31,37,47,53,55\} & b'=\{11,17,33,41,43,51\} & c'=\{35,49\} \end{array}$$

$$\begin{array}{lll} f=\{0\} & g=\{2,6,18,38,50,54\} & h=\{4,12,20,36,44,52\} \\ | & | & | \\ f'=\{28\} & g'=\{10,22,26,30\} & h'=\{8,16,24,32,40,48\} \end{array} \qquad \{14,42\}$$

As $D+28$, $29D$, $29D+28$ are all fixed by 3 and $29a' = a$, we may assume that

$$f \cup a = \{0,1,3,9,19,25,27\} \subset D,$$

$$(a' \cup f') \cup \{14,42\} \cap D = \emptyset.$$

Note that D will include exactly one orbit of each LL pair. Now we construct the characteristic graphs of the differences 2 and 4, as in Fig. 15.

Observing the number of occurrences of 2 and the number of occurrences of 4 in the difference list of each orbit, we find that

$$N'(G_{13}^w[D]) = N'(G_{13,1}^w[D]) + N'(G_{13,2}^w[D]) = 10, \quad w = 2, 4 \tag{6.20}$$

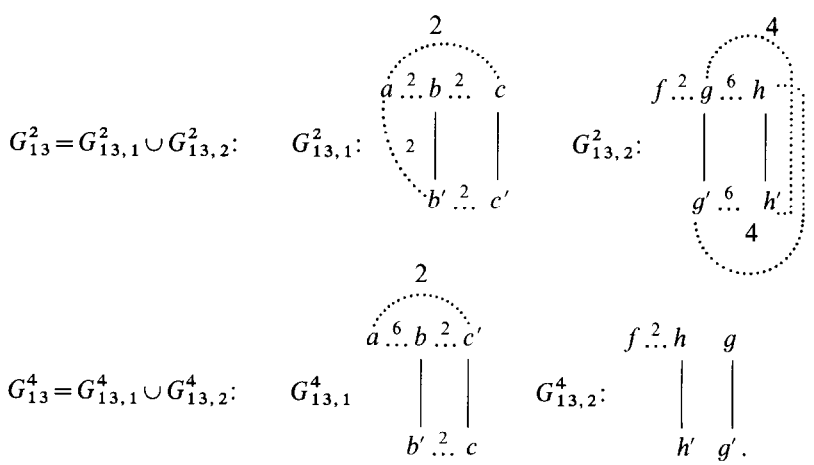


Fig. 15.

Table 8

$G^2_{13,1}[D]$	$N(G^2_{13,1}[D])$	$N(G^4_{13,1}[D])$
abc	6	8
abc'	2	8
$ab'c$	4	4
$ab'c'$	4	0

Table 9

$G^2_{13,2}[D]$	$N(G^2_{13,2}[D])$	$N(G^4_{13,2}[D])$
fgh	8	2
fgh'	6	0
$fg'h$	4	2
$fg'h'$	6	0

In Tables 8 and 9 we list out all the possible $G^2_{13,1}[D]$, $G^2_{13,2}$ and the corresponding $N(G^w_{13,1}[D])$ and $N(G^w_{13,2}[D])$, $w=2,4$. There are only two combinations of $G^2_{13,1}[D]$ and $G^2_{13,2}[D]$ satisfying (6.20):

(1) $D_1 = a \cup b \cup c \cup f \cup g \cup h$

$= \{0, 1, 3, 4, 5, 7, 9, 10, 12, 13, 15, 19, 20, 21, 22, 23, 25, 26, 27, 30, 34, 36,$

$39, 44, 45, 46, 52\},$

(2) $D_2 = a \cup b \cup c \cup f \cup g \cup h$

$= \{0, 1, 2, 3, 4, 5, 6, 9, 12, 13, 15, 18, 19, 20, 23, 25, 27, 35, 36, 38, 39, 44,$

$45, 49, 50, 52, 54\}.$

It can be checked that $D_1 = 5D_2$ and D_2 is a $(56, 27, 13)$ near difference set. This completes the proof. □

Lemma 6.13. $N(68, 33, 16) = 0$.

Proof. Suppose D is a $(68, 33, 16)$ near difference set in Z_{68}. Since $11^7 \equiv 3 \pmod{68}$, 3 is a multiplier of D by Theorem 2.1, and we may assume that 3 fixes D. The orbits of Z_{68} under the permutation $x \to 3x$ are

$$A_1 = \{1, 3, 7, 9, 11, 13, 23, 25, 27, 31, 33, 39, 49, 53, 63\}$$
$$|$$
$$A_2 = \{2, 15, 19, 29, 35, 37, 41, 43, 45, 47, 55, 57, 59, 61, 65, 67\} \quad \{17, 51\}$$
$$\{0\} \qquad A_3 = \{2, 6, 10, 14, 18, 22, 26, 30, 38, 42, 46, 50, 54, 58, 62, 66\}$$
$$| \qquad\qquad |$$
$$\{34\} \qquad A_4 = \{4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64\}$$

Clearly, $\{17, 51\}$ cannot be included in D. D includes exactly one orbit of each LL pair. We may assume that $D \in D$. Noting that $37A_2 = A_1$, we may further assume that $A_1 \subset D$. No matter which of A_3 and A_4 is included in D, 2 appears at most ten times in the difference list of D, contradicting with $\lambda = 16$. This completes the proof. □

$$\begin{array}{cccccc} \{0\} & \{3\} & \{6\} & \{9\} & \{12\} & \{15\} \\ | & | & | & | & | & | \\ \{36\} & \{39\} & \{42\} & \{45\} & \{48\} & \{51\} \\ & & & & & \\ \{18\} & \{21\} & \{24\} & \{27\} & \{30\} & \{33\} \\ | & | & | & | & | & | \\ \{54\} & \{57\} & \{60\} & \{63\} & \{66\} & \{69\}\,. \end{array} \tag{6.21}$$

Fig. 16.

Lemma 6.14. $N(72, 35, 17) = 0$.

Proof. Suppose that D is a $(72, 35, 17)$ difference set in Z_{72}. 25 is a multiplier of D, for $5^2 \equiv 7^4 \equiv 25 \pmod{72}$. We assume that 25 fixes D, then D is a union of some of the orbits of the form:

$$a\{1, 25, 49\}.$$

When $3 \nmid a$, $a \cdot \{1, 25, 49\}$ has length 3 and its difference list consists of three ± 24. When $3 \mid a$, $a \cdot \{1, 25, 49\}$ has length one; and all such orbits are given in Fig. 16. D includes at most one orbit of each LL pair in (6.18), so D includes at least eight orbits of length 3. Therefore, 24 would appear at least $3 \cdot 8 = 24$ times in the difference list of D, contradicting with $\lambda = 17$. This completes the proof. □

Acknowledgements

The authors wish to thank professor S.M. Dodunekov and Mr. Q. Xiang for their helpful comments.

References

[1] L.D. Baumert, Cyclic Difference Sets, Lecture Notes in Mathematics, Vol. 182 (Springer, New York, 1971).
[2] J.W.S. Cassels, On the equation $a^x - b^y = 1$, Amer. J. Math. 75 (1953) 159–162.
[3] J.E.H. Elliott and A.T. Butson, Relative difference sets, Illinois J. Math. 10 (1966) 517–531.
[4] D. Hughes, Biplanes and semi-biplanes, in: D.A. Holton and J. Sebery, eds., Lecture Notes in Mathematics, Vol. 688 (Springer, Berlin, 1978).
[5] C. Ko, On the Diophantine equation $x^2 = y^p + 1$, $xy \neq 0$, Sci. Sinica 14 (1964) 457–460.
[6] H.-P. Ko and D.K. Ray-Chaudhuri, Multiplier theorems, J. Combin. Theory Ser. A 30 (1981) 134–157.
[7] R.L. McFarland and B.F. Rice, Translates and multipliers of abelian difference sets, Proc. Amer. Math. Soc. 68 (1978) 375–379.
[8] L.J. Mordell, Diophantine Equations (Academic Press. New York, 1969).
[9] T. Nagell, Sur l' impossibiliti de lequation indeterminee $z^p + 1 = y^2$, Norsk Mat. Forenings Skrifter. **1** (4) (1921).
[10] H.J. Ryser, Variants of cyclic difference sets, Proc. Amer. Math. Soc. 41 (1973) 45–50.
[11] W.-D. Wei, Near difference sets of type 2 (Research announcement), Adv. in Math. 16 (1987) 327–328; J. Sichuan Univ. Natural Science Edition, 24 (1987) 391–396.